CLAIMS

What is claimed is:

1. A method of establishing a secured communication session across a remote network connection, comprising:

(a) receiving a first certificate that includes a first digital signature;

(b) obtaining a first public key;

(c) using the first public key to verify the first digital signature;

(d) if the first digital signature in (c) is successfully verified, receiving a second certificate that includes a second digital signature;

(e) obtaining a second public key; and

(f) using the second public key to verify the second digital signature.

2. The method of claim 1 wherein said first and second digital signatures are signed with different private keys.

3. The method of claim 1 wherein said second certificate includes at least a portion of said first certificate.

4. The method of claim 1 wherein (c) includes decrypting a portion of said first certificate to recover a first hash value.

5. The method of claim 4 wherein (c) also includes computing a hash of at least a portion of said first certificate to produce a first computed hash value.

6. The method of claim 5 wherein said first hash value is compared to said first computed hash value.

7. The method of claim 6 wherein (c) further includes determining said first digital signature is successfully verified if said first hash value matches said first computed hash value.

8. The method of claim 1 wherein (f) includes decrypting a portion of said second certificate to recover a second hash value.

9. The method of claim 8 wherein (f) also includes computing a hash of at least a portion of said second certificate to produce a second computed hash value.

10. The method of claim 9 wherein said second hash value is compared to said second computed hash value.

11. The method of claim 10 further including successfully verifying said second digital signature if said second hash value matches said second computed hash value.

12. A method of establishing a secured communication session across a remote network connection, comprising:

(a) receiving first and second certificates that include first and second digital signatures, respectively;

(b) obtaining first and second public keys;

(c) using the first public key to verify the first digital signature;

(d) if the first digital signature in (c) is successfully verified, verifying the second digital signature; and

(e) permitting the communication session to occur if both said first and said second digital signatures are successfully verified.

13. The method of claim 12 wherein said first and second digital signatures are signed with different private keys.

14. The method of claim 12 wherein said second certificate includes at least a portion of said first certificate.

15. The method of claim 12 wherein (c) includes using said first public key to decrypt a portion of said first certificate to recover a first hash value.

16. The method of claim 15 wherein (c) also includes computing a hash of at least a portion of said first certificate to produce a first computed hash value.

17. The method of claim 16 wherein (c) includes comparing said first hash value to said first computed hash value.

18. The method of claim 17 wherein (c) further includes determining that said first digital signature is successfully verified if said first hash value matches said first computed hash value.

19. The method of claim 12 wherein (c) includes decrypting a portion of said second certificate to recover a second hash value.

20. The method of claim 19 wherein (c) also includes computing a hash of at least a portion of said second certificate to produce a second computed hash value.

21. The method of claim 20 wherein (c) includes comparing said second hash value to said second computed hash value.

22. The method of claim 21 further including successfully verifying said second digital signature if said second hash value matches said second computed hash value.

23. A method of creating a remotely verifiable certificate, comprising:

(a) retrieving a first signed certificate;

(b) combining together said first signed certificate with other values;

(c) computing a hash of the combination from (b); and

(d) signing said hash from (c) with a private key.

24. The method of claim 23 wherein said other values in (b) includes an IP address.

25. The method of claim 23 wherein said other values in (b) includes a domain name.

26. A computer, comprising:

a processor; and

a memory coupled to said processor;

wherein said memory includes storage for a first certificate and a second certificate, said second certificate derived from said first certificate.

27. The computer system of claim 26 wherein said processor combines at least a portion of said first certificate with additional values, computes a hash of said combination, and encrypts said hash with a private key.

28. The computer system of claim 27 wherein said additional values include an IP address.

29. The computer system of claim 27 wherein said additional values include a domain name.

30. The computer system of claim 26 wherein said first certificate includes a serial number.

31. The computer system of claim 26 wherein said first certificate is not created by the server.

32. A client system, comprising:

a processor; and

a memory coupled to said processor; and

a connection to a communication link to a server;

wherein said processor requests a first certificate from the server, verifies a first digital signature associated with said first certificate, and if said first digital signature is successfully verified, requests a second certificate from said server and verifies a second digital signature associated with said second certificate.

33. The client system of claim 32 wherein the client uses two different public keys to verify the first and second digital signatures.

34. A client system, comprising:

a processor;

a memory coupled to said processor; and

a connection to a communication link to a server;

wherein said processor requests a first certificate and a second certificate from the server, verifies a first digital signature associated with said first certificate, and if said first digital signature is successfully verified, verifies a second digital signature associated with said second certificate.

35. The client system of claim 34 wherein the client uses two different public keys to verify the first and second digital signatures.